AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of the claims in the application:

1-43. (Canceled)

44. (Currently Amended) A method including the following:

at a certification authority, receiving an executable program generated by a party independent of the certification authority;

~~at the certification authority, determining that no specification is available to the certification authority adequately describing the operations of the executable program;~~

at the certification authority, testing the executable program and, based on the results of the testing, generating a specification describing the actual operation of the executable program; and

at the certification authority, generating a digital certificate certifying that the executable program operates in the manner described in the specification.

45. (Currently Amended) A method as in claim 44, further including:

receiving the executable program at a user site;

receiving the digital certificate at the user site;

at the user site, evaluating the digital certificate to determine if the digital certificate is associated with the executable program;

at the ~~site~~ user site, evaluating the digital certificate to determine whether to execute the executable program; and

at the user site, executing the executable program, the execution being dependent on the evaluation of the digital certificate.

46. (Previously Presented) A method as in claim 45, in which:
the digital certificate specifies a security level, and
the user site evaluation of the digital certificate to determine whether to execute the executable program includes comparing the security level to a required security level.

47. (Currently Amended) A method as in claim 45, in which:
the user site evaluation of the digital certificate to determine if the digital certificate is associated with the executable program includes comparing a hash value stored in the digital certificate to a hash of at least a portion of the executable program.

48. (Currently Amended) A method as in claim 47, in which:
the hash value comparison is preceded by the user site decrypting the hash value stored in the digital certificate using a public key associated with the certification authority.

49. (Previously Presented) A method as in claim 45, in which:
the digital certificate includes the specification, and the step of evaluating the digital certificate to determine whether to execute the executable program includes evaluating the specification.

50. (New) A method as in claim 45, in which the user site includes a tamper-resistant execution space, the tamper-resistant execution space being operable to protect against tampering, by a user at the user site, with the performance of said step of evaluating the digital certificate to determine whether to execute the executable program.

51. (New) A method as in claim 45, in which the executable program is received at the user site in encrypted form, the method further comprising:
decrypting the executable program.

52. (New) A method as in claim 51, in which the user site includes a tamper-resistant execution space, the tamper-resistant execution space being operable to protect against tampering, by a user at the user site, with the performance of said steps of (i) decrypting the executable program, and (ii) evaluating the digital certificate to determine whether to execute the executable program.

53. (New) A method as in claim 50, in which the tamper-resistant execution space includes a secure processing unit.

54. (New) A computer readable medium containing executable program instructions, the executable program instructions including instructions for:

receiving an executable program from a third party;

testing the executable program and, based on the results of the testing, generating a specification describing the actual operation of the executable program; and

generating a digital certificate certifying that the executable program operates in the manner described in the specification.

55. (New) A computer readable medium as in claim 54, further including instructions for:

sending the executable program to a user site.

56. (New) A computer readable medium as in claim 54, further including instructions for:

sending the digital certificate to a user site.

57. (New) A computer readable medium as in claim 54, further including instructions for:

sending the specification to a user site.

58. (New) A computer readable medium as in claim 54, further including instructions for:

encrypting the executable program.

59. (New) A system comprising:

means for receiving an executable program;

means for testing the executable program and, based on the results of the testing, generating a specification describing the actual operation of the executable program; and

means for generating a digital certificate certifying that the executable program operates in the manner described in the specification.

60. (New) A system as in claim 59, further comprising:

means for sending the executable program to a user site.

61. (New) A system as in claim 59, further comprising:

means for sending the digital certificate to a user site.

62. (New) A system as in claim 59, further comprising:

means for sending the specification to a user site.

63. (New) A system as in claim 59, further comprising:

means for encrypting the executable program.